

# Release A CDR RID Report

**Date Last Modified** 9/28/95  
**Originator** Art Gaylord  
**Organization** Univ. of Mass  
**E Mail Address** art@cs.umass.edu  
**Document** Security Architecture

**Phone No** (413) 545-2520

<b>RID ID</b>	<b>CDR</b>	35
<b>Review</b>	SDPS/CSMS	
<b>Originator Ref</b>		
<b>Priority</b>	1	

**Section**

**Page** LK-8

**Figure Table**

**Category Name** ECS System-Level

**Actionee** Project (Herring)

**Sub Category** Project

**Subject** Lack of an overall EOSDIS security plan.

## **Description of Problem or Suggestion:**

There is no EOSDIS security plan upon which to base implementation decisions or operational decisions. This leads to inconsistencies in security protection throughout the system. Equally important it can lead to inconsistencies in security protection throughout the system. Equally important, it can lead to difficulties in resolving security "incidents" and misunderstands between the various organizations with respect to where responsibilities lie.

## **Originator's Recommendation**

Develop and publish a security plan and ensure that the design implements it.

**GSFC Response by:** Ellen L Herring

**GSFC Response Date** 9/25/95

RID 35: ESDIS SYSTEM SECURITY PLAN

The ESDIS Project agrees that an overall plan for ESDIS system security should be produced. To accomplish this task the following activities will take place:

1)A document will be produced that establishes EOSDIS security policy and guidance. It will include an overview of the security requirements, including the level of security requirements to be met within a particular EOSDIS facility, system or interface. It will provide a description of how the security requirements are allocated throughout the ground system elements with pointers to security plans that identify specific security implementations for the individual elements. The EOSDIS policy will have minor impact on existing ECS, EBnet and EDOS design since each component's security plan uses the same NASA security document (NHB2410) as a reference.

2)A security working group or tiger team will be established to refine details that cross security policy boundaries. The security working group will consist of representatives from EOSDIS components (ECS,EBnet,etc.) to ensure compliance and consistency across individual organization security plans. The working group will also facilitate concurrent updates to individual organization plans as the EOSDIS policy/guidance is formulated.

## **SCHEDULE**

1. Annotated Security Plan Outline/15 October 1995
2. Policy (Baseline)/30 November 1995
3. Plan Rough Draft/12 January 1996
4. Security Plan (Final)/9 February 1996
5. System Risk Analysis/Risk Management Plan/April 1996

**HAIS Response by:**

**HAIS Schedule**

**HAIS R. E.**

**HAIS Response Date**

**Status** Closed

**Date Closed** 9/28/95

**Sponsor** Schroeder

\*\*\*\*\* Attachment if any \*\*\*\*\*

\*\*\*\*\* Attachment, if any \*\*\*\*\*  
**Release A CDR RID Report**

---